PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Attorney Docket No. 555255012714

In re Application of	:	Herbert A. Little; et al.
Serial No.	:	10/817,070
Filing Date	:	04/02/2004
For	:	SYSTEM AND METHOD OF ACCESSING KEYS FOR SECURE MESSAGING
Art Unit	:	2109
Examiner	:	Martin Jeriko P. San Juan

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

This Appeal Brief is being submitted with the Notice of Appeal having been filed on August 5, 2008. The Commissioner is hereby authorized to charge any necessary fees and credit any overpayment associated with this Appeal to Jones Day Deposit Account No. 501432, ref: 555255-012714.

I. Real Parties In Interest

The real party in interest is Research In Motion Limited, as evidenced by the assignment recorded at Reel/Frame 015192/0760.

II. Related Appeals And Interferences

There are no related appeals or interferences to the instant application.

III. Status Of Claims

Claims 1-22 and 25-27 are pending and are finally rejected. Claims 23 and 24 have been cancelled without prejudice. The specific rejections of claims 1, 3, 8, and 25-27 are hereby appealed. The rejections of the remaining claims stand or fall with the rejection of their respective independent claims.

IV. Status Of Amendments

There have been no amendments filed since the Final Office Action of February 5, 2008.

V. Summary Of Claimed Subject Matter

The claimed subject matter generally relates to handling on a wireless mobile communication device a secure message to be sent from the wireless mobile communication device to a recipient. Data is received about a security key that is associated with the recipient. The data is then used to perform a validity check related to sending the secure message to the recipient. The validity check may uncover an issue related to sending the secure message to the

recipient. If an issue is uncovered, a reason is determined for the validity check issue and is provided via a user interface on the device.

Such processing on a sender's device with respect to sending secure messages can be helpful in many situations. For example, this processing provides a user of the device the benefit of taking steps to ameliorate a validity check issue before the secure message is even sent. This is in contrast to previous approaches which provided only a limited notification when an error has been encountered in accessing a key (e.g., a public key) required for secure communications.

A. Independent Claim 1

Claim 1 is directed to a method for handling on a wireless mobile communication device a secure message to be sent from the wireless mobile communication device to a recipient. In claim 1, data is received at the wireless mobile communication device about a security key associated with the recipient. The received data is used to perform a validity check with respect to using the security key associated with the recipient to send a secure message to the recipient. If an issue exists due to the validity check, a reason is determined for the validity check issue. The reason for the validity check issue is provided via a user interface on the mobile device.

As mentioned above, claim 1 recites receiving data at the wireless mobile communication device about a security key associated with the recipient. An example of this claim limitation is described in the assignee's specification at page 12 (line 23) to page 13 (line 11).

Still further, claim 1 recites using the received data to perform a validity check with respect to using the security key associated with the recipient to send a secure message to the recipient. An example of this claim limitation is described in the assignee's specification at page 13 (line 20) to page 14 (line 15) and at page 15 (lines 5-10).

Still further, claim 1 recites that an issue exists due to the validity check and determining a reason for the validity check issue. An example of these claim limitations is described in the assignee's specification at page 13 (lines 16-19).

Still further, claim 1 recites that the reason for the validity check issue is provided via a user interface on the mobile device. An example of this claim limitation is described in the assignee's specification at page 12 (lines 20-22) and at page 17 (line 20) to page 18 (line 5).

B. Dependent Claim 3

Claim 3 depends from claim 1 and recites resolving the validity check issue through use of the information provided in the validity check reason, wherein the secure message is sent after resolution of the validity check issue by the user. An example of these limitations is shown in the specification at page 13 (lines 16-19).

C. Dependent Claim 8

Claim 8 depends indirectly from claim 1 and recites canceling sending the message to a recipient whose certificate was not located. An example of this limitation is shown in the specification at page 14 (lines 8-9).

D. Independent Claim 25

Claim 25 is directed to handling on an electronic device a secure message to be sent from the electronic device to a recipient. In claim 25, a secure message processing module is used with a messaging client to send electronic messages to recipients. The secure message processing module receives data about a security key associated with the recipient. The secure

message processing module uses the received data to perform a validity check with respect to using the security key associated with the recipient to send a secure message to the recipient. If an issue exists based upon the validity check, the secure message processing module determines a reason for the validity check issue. The secure message processing module provides the reason for the validity check issue via a user interface of the electronic device.

As mentioned above, claim 25 recites a secure message processing module for use with a messaging client that sends electronic messages to recipients and for receiving data about a security key associated with the recipient. An example of these claim limitations is described in the assignee's specification at page 12 (line 14) to page 13 (line 11).

Still further, claim 25 recites that the secure message processing module uses the received data to perform a validity check with respect to using the security key associated with the recipient to send a secure message to the recipient. An example of this claim limitation is described in the assignee's specification at page 13 (line 20) to page 14 (line 15) and at page 15 (lines 5-10).

Still further, claim 25 recites that an issue exists based upon the validity check and a reason is determined for the validity check issue. An example of these claim limitations is described in the assignee's specification at page 13 (lines 16-19).

Still further, claim 25 recites that the reason for the validity check issue is provided via a user interface on the electronic device. An example of this claim limitation is described in the assignee's specification at page 12 (lines 20-22) and at page 17 (line 20) to page 18 (line 5).

E. Independent Claim 26

Claim 26 is directed to a wireless mobile communication device that handles a secure message to be sent from the wireless mobile communication device to a recipient. In claim 26, the device includes a certificate store to store certificate data and means for using the stored certificate data to perform a validity check with respect to using the recipient's security key for sending the secure message to the recipient. If an issue exists due to the validity check, then a reason is determined for the validity check issue. The reason for the validity check issue is provided via a user interface of the mobile device.

As mentioned above, claim 26 recites a certificate store to store certificate data and means for using the stored certificate data to perform a validity check with respect to using the recipient's security key for sending the secure message to the recipient. An example of these claim limitations is described in the assignee's specification at page 12 (line 23) to page 13 (line 11), at page 13 (line 20) to page 14 (line 15), and at page 15 (lines 5-10).

Still further, claim 26 recites that an issue exists due to the validity check and means for determining a reason for the validity check issue. An example of these claim limitations is described in the assignee's specification at page 13 (lines 16-19).

Still further, claim 26 recites means for providing the reason for the validity check issue via a user interface of the mobile device. An example of this claim limitation is described in the assignee's specification at page 12 (lines 20-22) and at page 17 (line 20) to page 18 (line 5).

F. Independent Claim 27

Claim 27 is directed to a computer-readable storage medium encoded with instructions to handle on a wireless mobile communication device a secure message to be sent from the wireless

mobile communication device to a recipient. In claim 27, data is received at the wireless mobile communication device about a security key associated with the recipient. The received data is used to perform a validity check with respect to using the security key associated with the recipient to send a secure message to the recipient. If an issue exists due to the validity check, a reason is determined for the validity check issue. The reason for the validity check issue is provided via a user interface on the mobile device.

As mentioned above, claim 27 recites receiving data at the wireless mobile communication device about a security key associated with the recipient. An example of this claim limitation is described in the assignee's specification at page 12 (line 23) to page 13 (line 11).

Still further, claim 27 recites using the received data to perform a validity check with respect to using the security key associated with the message recipient to send a secure message to the recipient. An example of this claim limitation is described in the assignee's specification at page 13 (line 20) to page 14 (line 15) and at page 15 (lines 5-10).

Still further, claim 27 recites that an issue exists due to the validity check and determining a reason for the validity check issue. An example of these claim limitations is described in the assignee's specification at page 13 (lines 16-19).

Still further, claim 27 recites that the reason for the validity check issue is provided via a user interface on the mobile device. An example of this claim limitation is described in the assignee's specification at page 12 (lines 20-22) and at page 17 (line 20) to page 18 (line 5).

VI. Grounds Of Rejection To Be Reviewed On Appeal

Claims 1, 3, 8, and 25-27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable

over U.S. Publication No. 2002/0169954, application of Bandini, et al. (Bandini) in view of U.S. Patent No. 6,782,266, issued to Baer, et al. (Baer). These rejections are appealed.

VII. Argument

A. Claim 1 Is Patentable Over Bandini and Baer

Claim 1 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Publication No. 2002/0169954, application of Bandini, et al. (Bandini) in view of U.S. Patent No. 6,782,266, issued to Baer, et al. (Baer). The rejection of claim 1 as being unpatentable over the cited references is improper because the cited references do not teach the following limitations of claim 1:

- *using the received data to perform a validity check with respect to using the security key associated with the recipient to send a secure message to the recipient;*
- *wherein the reason for the validity check issue is provided via a user interface on the mobile device.*

1. Neither Reference Teaches Claim 1's Limitation Of Providing A Reason For A Validity Check Issue Via A User Interface On A Mobile Device.

Claim 1 of the instant application is directed to a method for handling on a wireless mobile communication device a secure message to be sent from the wireless mobile communication device to a recipient. Claim 1 specifically recites that *the reason for the validity check issue is provided via a user interface on the mobile device.* In rejecting this subject matter of claim 1, the Final Office Action cites paragraph 44 of Bandini, which reads:

> Turning to FIG. 6(a), at 602, the e-mail firewall 105 determines if decryption of portions of the message 204 is required. If so, then at 604, decryption is performed in accordance with stored private keys 628. Storing private keys is well known in the art of public key cryptography. After decryption, or if no decryption is required, the e-mail firewall 105 applies policy managers 216, which can perform four types of actions (shown at 610, 612, 614, 616, and 620) on e-mail message 204 for each policy. Criteria actions 610 present filtering criteria selected by the administrator. Exception actions 612 determine which criteria 610 are excluded. Multiple criteria 610 can be selected which effectively results in a logical AND operation of the criteria. Multiple exceptions 612 can be selected which effectively results in a logical OR operation of the exceptions; that is, any one of the exception conditions being true will result in a policy not being triggered. In another embodiment, a generic Boolean expression is used in lieu of the criteria and exception combination. Annotation actions 614 cause generation of attachment to message 602 or insertion of text into the body 208 of the message. The manner by which annotations are made is based on a policy entered by the administrator. Notification actions 616 cause the sending of one or more e-mail notifications when a given policy is triggered. Notifications can be sent to sender, recipient, administrator, or any e-mail address that is defined by the administrator. In addition, notification actions 616 allow specification of whether the original message 204 should accompany the notification. Disposition action 620 determines whether the message should continue to the destination(s) (specified by field 620) or whether one of a plurality of alternative actions 622 such as deferral, quarantine, return to sender, or dropping of the message are required.

The cited passage, however, does not teach the subject matter of claim 1, namely that a reason is determined for the issue resulting from the validity check and that reason is provided to the user of a mobile device. Bandini is only disclosing notification that an issue has arisen and does not provide any functionality for providing the underlying reason behind the issue. Because Bandini does not teach a method of determining the reason for an issue that has arisen at the device and providing that reason to the user of a mobile device, the user has greater difficulty in taking corrective action with respect to the issue. The simple notification in Bandini that an issue exists results in a significantly less efficient approach in allowing a mobile user to take

ameliorative action, such as to take corrective action more quickly in order to allow the anticipated communication to take place once the issue is resolved.

The examiner "acknowledges" the assignee's concerns that Bandini does not teach determining a reason for the issue resulting from the validity check. (See, Final Office Action, page 3.) However, the Final Office Action then cites paragraphs 45-47 of Bandini as teaching this limitation of claim 1, stating that the cited paragraphs provide "an example of a policy being triggered which provides further evidence of the extent of information that is included in the annotation and notification actions." (See, Final Office Action, page 3.) The office action's response to the assignee's argument further states:

> In the end of the execution of a policy being triggered, Bandini discloses that "the security manager provides a corresponding result notification to the policy manager so as to facilitate proper follow up actions, such as rejection or acceptance of the e-mail message (Par 0047)." This is evidence of the extent of information that is included in the Annotation, Notification actions of a Policy Manager whenever a policy issue has arisen. The extent of information that is included in the annotation/notification suggests or implies "a reason(s) for any validity check issues," since "corresponding result notification" would have suggested or implied to include information of any point of failures that have occurred during the execution of a policy, "so as to facilitate proper follow up actions, such as rejection or acceptance of the e-mail message." (See, Final Office Action, pages 3-4; Emphasis in the original.)

The assignee respectfully disagrees with the office action's characterization of paragraphs 45-47 of Bandini. The "result notification" mentioned in Bandini is provided to ***the policy manager software module*** to facilitate follow-up actions. Even *assuming arguendo* that Bandini "suggests or implies" a reason for a validity check issue (which it does not), Bandini includes no teaching whatsoever of providing a reason for a validity check issue via ***a user interface on a mobile device***, as required by claim 1. Because in claim 1 the reason for the validity check issue is surfaced to the user, the user can take corrective action before the message is even sent.

The examiner further maintains that Bandini discloses "surfacing the validity check to the user so that the user can take corrective action before the message is even sent" based upon the following passage from paragraph 44: "[d]isposition action 620 determines whether the message should continue to the destination(s)." (See, Advisory Action dated June 16, 2008, page 2.) However contrary to this position, the "disposition action" at step 620 in the flowchart of figure 6(a) is being performed by the e-mail firewall and not by the user. This is made clear in multiple locations in Bandini: "FIG. 6(a) [which includes step 620] is a flowchart showing ***operation of the e-mail firewall*** 105 in response to a received message" (see, paragraph 43 of Bandini; emphasis added); and paragraph 15 of Bandini identifies figure 6(a) as "illustrating operation of the preferred embodiment of an e-mail firewall." Accordingly, any alleged corrective action in the cited passage of Bandini is being performed by the e-mail firewall and not by the user. Whether an electronic messaging reader is a type of user-interface (as maintained in the Advisory Action) is immaterial since, as shown above, Bandini discloses that it is the e-mail firewall performing the alleged corrective action and not the user. Since neither Bandini (nor any of the other cited references) teach the aforementioned limitation of claim 1, claim 1 is allowable and should proceed to issuance.

2. Neither Reference Teaches That The Processing Performed With Respect To A Secure Message Occurs Before A Message Is Even Sent.

Claim 1 of the instant application requires that processing of the secure message occurs before a message is even sent. This provides a user of the mobile device the benefit of taking steps to ameliorate the validity check issue before the secure message is sent. (As an example,

dependent claim 8, which is argued below, further emphasizes this aspect by allowing a user to cancel the sending of the message to a recipient whose certificate was not located.)

Claim 1 makes clear that the processing of the secure message occurs before the message is sent, such as in the preamble (emphasis added): "*A method for handling on a wireless mobile communication device a secure message to be sent from the wireless mobile communication device to a recipient*." Claim 1 further recites steps about a secure message that is to be sent (i.e., the secure message has not been sent yet), such as the following step (emphasis added): "*using the received data to perform a validity check with respect to using the security key associated with the recipient to send a secure message to the recipient*."

The Final Office Action cites paragraph 44 of Bandini as disclosing this aspect of claim 1. However, paragraph 44 of Bandini is explicitly directed to the handling of e-mail messages that have already been sent by the user. Paragraph 44 discusses Figure 6(a) of Bandini. As Bandini states, "FIG. 6(a) is a flowchart showing operation of the e-mail firewall 105 in response to a ***received message***." (See, paragraph 43 of Bandini; emphasis added.) In Bandini, an e-mail firewall receives a message that has already been sent from a sender.

The Advisory Action further argues that processing is performed before a message is sent by maintaining that the processing of the message in Bandini is performed before it has been delivered to the intended recipient. The assignee respectfully submits that this is an incorrect position. In general, a message is sent when a sender has activated the message send button and the message leaves the device. In Bandini, the e-mail message has already left the sender and is now being processed by the e-mail firewall as shown by the flowcharts of figures 6(a) and 6(b). Since neither Bandini (nor any of the other cited references) teach the aforementioned feature of claim 1, claim 1 is allowable and should proceed to issuance.

B. Dependent Claim 3 Is Patentable Over Bandini and Baer

Claim 3 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Publication No. 2002/0169954, application of Bandini, et al. (Bandini) in view of U.S. Patent No. 6,782,266, issued to Baer, et al. (Baer). Claim 3 depends from claim 1 and reads as follows:

> 3. The method of claim 1, further comprising the step of resolving the validity check issue through use of the information provided in the validity check reason, wherein the secure message is sent after resolution of the validity check issue by the user.

Dependent claim 3 recites that the user of the mobile device is allowed to resolve the issue resulting from the validity check, after which the secure message may be sent. In rejecting this claim, the office action cites paragraphs 44 and 64 of Bandini, stating that "[d]isposition or alternative actions, after a notification action, are available for the sender." For example, the message dispositions or alternative actions include "deferral, quarantine, return to sender, or dropping of the message as required." (See, paragraph 44 of Bandini.) However, none of the dispositions or alternative actions are related to resolving a "validity check reason" as required by claim 3. Since neither Bandini (nor any of the other cited references) teach the aforementioned feature of claim 3, claim 3 is allowable and should proceed to issuance.

C. Dependent Claim 8 Is Patentable Over Bandini and Baer

Claim 8 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Publication No. 2002/0169954, application of Bandini, et al. (Bandini) in view of U.S. Patent No. 6,782,266, issued to Baer, et al. (Baer). Claim 8 depends indirectly from claim 1 and reads as follows:

8. The method of claim 6 further comprising the step of canceling sending the message to a recipient whose certificate was not located.

As mentioned above with respect to claim 1 above, processing is performed with respect to a secure message before a message is even sent to the recipient. This aspect allows the feature of dependent claim 8 to exist, namely to provide the feature of canceling sending the message to the recipient in case of a problem (i.e., the recipient's certificate cannot be located). This provides a user of the mobile device the benefit of taking steps to ameliorate the validity check problem before the secure message is even sent, such as the step in dependent claim 8 of canceling the sending of the message to a recipient.

The Final Office Action cites paragraph 64 of Bandini as disclosing this feature of claim 8. However, this paragraph of Bandini discloses actions that occur at an e-mail firewall after a message has already been sent, and thus the ameliorative action of claim 8 of canceling the sending of the message cannot be performed. Since neither Bandini (nor any of the other cited references) teach the aforementioned feature of claim 8, claim 8 is allowable and should proceed to issuance.

D. Claim 25 Is Patentable Over Bandini and Baer

Claim 25 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Publication No. 2002/0169954, application of Bandini, et al. (Bandini) in view of U.S. Patent No. 6,782,266, issued to Baer, et al. (Baer). The rejection of claim 25 as being unpatentable over the cited references is improper because the cited references do not teach the following limitations of claim 25:

- *wherein the secure message processing module uses the received data to perform a validity check with respect to using the security key associated with the recipient to send a secure message to the recipient;*
- *wherein the secure message processing module provides the reason for the validity check issue via a user interface of the electronic device.*

1. Neither Reference Teaches Claim 25's Limitation Of Providing A Reason For A Validity Check Issue Via A User Interface On An Electronic Device.

Claim 25 of the instant application is directed to handling on an electronic device a secure message to be sent from the electronic device to a recipient. Claim 25 specifically recites that *the secure message processing module provides the reason for the validity check issue via a user interface of the electronic device*. In rejecting this subject matter of claim 25, the Final Office Action cites paragraph 44 of Bandini, which reads:

> Turning to FIG. 6(a), at 602, the e-mail firewall 105 determines if decryption of portions of the message 204 is required. If so, then at 604, decryption is performed in accordance with stored private keys 628. Storing private keys is well known in the art of public key cryptography. After decryption, or if no decryption is required, the e-mail firewall 105 applies policy managers 216, which can perform four types of actions (shown at 610, 612, 614, 616, and 620) on e-mail message 204 for each policy. Criteria actions 610 present filtering criteria selected by the administrator. Exception actions 612 determine which criteria 610 are excluded. Multiple criteria 610 can be selected which effectively results in a logical AND operation of the criteria. Multiple exceptions 612 can be selected which effectively results in a logical OR operation of the exceptions; that is, any one of the exception conditions being true will result in a policy not being triggered. In another embodiment, a generic Boolean expression is used in lieu of the criteria and exception combination. Annotation actions 614 cause generation of attachment to message 602 or insertion of text into the body 208 of the message. The manner by which annotations are made is based on a policy entered by the administrator. Notification actions 616 cause the sending of one or more e-mail notifications when a given policy is triggered. Notifications can be

> sent to sender, recipient, administrator, or any e-mail address that is defined by the administrator. In addition, notification actions 616 allow specification of whether the original message 204 should accompany the notification. Disposition action 620 determines whether the message should continue to the destination(s) (specified by field 620) or whether one of a plurality of alternative actions 622 such as deferral, quarantine, return to sender, or dropping of the message are required.

The cited passage, however, does not disclose the subject matter of claim 25, namely that a reason is determined for the issue resulting from the validity check and that reason is provided to the user of an electronic device. Bandini is only disclosing notification that an issue has arisen and does not provide any functionality for providing the underlying reason behind the issue. Because Bandini does not disclose a determining the reason for an issue that has arisen at the device and providing that reason to the user of the device, the user has greater difficulty in taking corrective action with respect to the issue. The simple notification in Bandini that an issue exists results in a significantly less efficient approach in allowing a user to take ameliorative action, such as to take corrective action more quickly in order to allow the anticipated communication to take place once the issue is resolved.

The examiner "acknowledges" the assignee's concerns that Bandini does not disclose determining a reason for the issue resulting from the validity check. (See, Final Office Action, page 3.) However, the Final Office Action then cites paragraphs 45-47 of Bandini as teaching this limitation of claim 25, stating that the cited paragraphs provide "an example of a policy being triggered which provides further evidence of the extent of information that is included in the annotation and notification actions." (See, Final Office Action, page 3.) The office action's response to the assignee's argument further states:

> In the end of the execution of a policy being triggered, Bandini discloses that "the security manager provides a corresponding result notification to the policy manager so as to facilitate proper follow up actions, such as

> rejection or acceptance of the e-mail message (Par 0047)." This is evidence of the extent of information that is included in the Annotation, Notification actions of a Policy Manager whenever a policy issue has arisen. The extent of information that is included in the annotation/notification suggests or implies "a reason(s) for any validity check issues," since "corresponding result notification" would have suggested or implied to include information of any point of failures that have occurred during the execution of a policy, "so as to facilitate proper follow up actions, such as rejection or acceptance of the e-mail message." (See, Final Office Action, pages 3-4; Emphasis in the original.)

The assignee respectfully disagrees with the office action's characterization of paragraphs 45-47 of Bandini. The "result notification" mentioned in Bandini is provided to ***the policy manager software module*** to facilitate follow-up actions. Even *assuming arguendo* that Bandini "suggests or implies" a reason for a validity check issue (which it does not), Bandini includes no teaching whatsoever of providing a reason for a validity check issue via ***a user interface of the electronic device***, as required by claim 25. Because in claim 25 the reason for the validity check issue is surfaced to the user, the user can take corrective action before the message is even sent.

The examiner further maintains that Bandini discloses "surfacing the validity check to the user so that the user can take corrective action before the message is even sent" based upon the following passage from paragraph 44: "[d]isposition action 620 determines whether the message should continue to the destination(s)." (See, Advisory Action dated June 16, 2008, page 2.) However contrary to this position, the "disposition action" at step 620 in the flowchart of figure 6(a) is being performed by the e-mail firewall and not by the user. This is made clear in multiple locations in Bandini: "FIG. 6(a) [which includes step 620] is a flowchart showing ***operation of the e-mail firewall*** 105 in response to a received message" (see, paragraph 43 of Bandini; emphasis added); and paragraph 15 of Bandini identifies figure 6(a) as "illustrating operation of the preferred embodiment of an e-mail firewall." Accordingly, any alleged corrective action in

the cited passage of Bandini is being performed by the e-mail firewall and not by the user. Whether an electronic messaging reader is a type of user-interface (as maintained in the Advisory Action) is immaterial since, as shown above, Bandini discloses that it is the e-mail firewall performing the alleged corrective action and not the user. Since neither Bandini (nor any of the other cited references) disclose the aforementioned limitation of claim 25, claim 25 is allowable and should proceed to issuance.

2. Neither Reference Teaches That The Processing Performed With Respect To A Secure Message Occurs Before A Message Is Even Sent.

Claim 25 of the instant application requires that processing of the secure message occurs before a message is even sent. This provides a user of the electronic device the benefit of taking steps to ameliorate the validity check issue before the secure message is sent.

Claim 25 makes clear that the processing of the secure message occurs before the message is sent, such as in the preamble (emphasis added): "*An apparatus for handling on an electronic device a secure message to be sent from the electronic device to a recipient.*" Claim 25 further recites limitations about a secure message that is to be sent (i.e., the secure message has not been sent yet), such as the following limitation (emphasis added): "*wherein the secure message processing module uses the received data to perform a validity check with respect to using the security key associated with the recipient to send a secure message to the recipient.*"

The Final Office Action cites paragraph 44 of Bandini as disclosing this aspect of claim 25. However, paragraph 44 of Bandini is explicitly directed to the handling of e-mail messages that have already been sent by the user. Paragraph 44 discusses Figure 6(a) of Bandini. As Bandini states, "FIG. 6(a) is a flowchart showing operation of the e-mail firewall 105 in response

to a ***received message***." (See, paragraph 43 of Bandini; emphasis added.) In Bandini, an e-mail firewall receives a message that has already been sent from a sender.

The Advisory Action further argues that processing is performed before a message is sent by maintaining that the processing of the message in Bandini is performed before it has been delivered to the intended recipient. The assignee respectfully submits that this is an incorrect position. In general, a message is sent when a sender has activated the message send button and the message leaves the device. In Bandini, the e-mail message has already left the sender and is now being processed by the e-mail firewall as shown by the flowcharts of figures 6(a) and 6(b). Since neither Bandini (nor any of the other cited references) disclose the aforementioned feature of claim 25, claim 25 is allowable and should proceed to issuance.

E. Claim 26 Is Patentable Over Bandini and Baer

Claim 26 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Publication No. 2002/0169954, application of Bandini, et al. (Bandini) in view of U.S. Patent No. 6,782,266, issued to Baer, et al. (Baer). The rejection of claim 26 as being unpatentable over the cited references is improper because the cited references do not disclose the following limitations of claim 26:

- *means for using the stored certificate data to perform a validity check with respect to using the recipient's security key for sending the secure message to the recipient;*
- *means for providing the reason for the validity check issue via a user interface of the mobile device.*

1. Neither Reference Teaches Claim 26's Limitation Of Providing A Reason For A Validity Check Issue Via A User Interface On A Mobile Device.

Claim 26 of the instant application is directed to handling on a wireless mobile communication device a secure message to be sent from the wireless mobile communication device to a recipient. Claim 26 specifically recites *means for providing the reason for the validity check issue via a user interface of the mobile device*. In rejecting this subject matter of claim 26, the Final Office Action cites paragraph 44 of Bandini, which reads:

> Turning to FIG. 6(a), at 602, the e-mail firewall 105 determines if decryption of portions of the message 204 is required. If so, then at 604, decryption is performed in accordance with stored private keys 628. Storing private keys is well known in the art of public key cryptography. After decryption, or if no decryption is required, the e-mail firewall 105 applies policy managers 216, which can perform four types of actions (shown at 610, 612, 614, 616, and 620) on e-mail message 204 for each policy. Criteria actions 610 present filtering criteria selected by the administrator. Exception actions 612 determine which criteria 610 are excluded. Multiple criteria 610 can be selected which effectively results in a logical AND operation of the criteria. Multiple exceptions 612 can be selected which effectively results in a logical OR operation of the exceptions; that is, any one of the exception conditions being true will result in a policy not being triggered. In another embodiment, a generic Boolean expression is used in lieu of the criteria and exception combination. Annotation actions 614 cause generation of attachment to message 602 or insertion of text into the body 208 of the message. The manner by which annotations are made is based on a policy entered by the administrator. Notification actions 616 cause the sending of one or more e-mail notifications when a given policy is triggered. Notifications can be sent to sender, recipient, administrator, or any e-mail address that is defined by the administrator. In addition, notification actions 616 allow specification of whether the original message 204 should accompany the notification. Disposition action 620 determines whether the message should continue to the destination(s) (specified by field 620) or whether one of a plurality of alternative actions 622 such as deferral, quarantine, return to sender, or dropping of the message are required.

The cited passage, however, does not disclose the subject matter of claim 26, namely that a reason is determined for the issue resulting from the validity check and that reason is provided to the user of a mobile device. Bandini is only disclosing notification that an issue has arisen and does not provide any functionality for providing the underlying reason behind the issue. Because Bandini does not disclose determining the reason for an issue that has arisen at the mobile device and providing that reason to the user of a mobile device, the user has greater difficulty in taking corrective action with respect to the issue. The simple notification in Bandini that an issue exists results in a significantly less efficient approach in allowing a mobile user to take ameliorative action, such as to take corrective action more quickly in order to allow the anticipated communication to take place once the issue is resolved.

The examiner "acknowledges" the assignee's concerns that Bandini does not disclose determining a reason for the issue resulting from the validity check. (See, Final Office Action, page 3.) However, the Final Office Action then cites paragraphs 45-47 of Bandini as teaching this limitation of claim 26, stating that the cited paragraphs provide "an example of a policy being triggered which provides further evidence of the extent of information that is included in the annotation and notification actions." (See, Final Office Action, page 3.) The office action's response to the assignee's argument further states:

> In the end of the execution of a policy being triggered, Bandini discloses that "the security manager provides a corresponding result notification to the policy manager so as to facilitate proper follow up actions, such as rejection or acceptance of the e-mail message (Par 0047)." This is evidence of the extent of information that is included in the Annotation, Notification actions of a Policy Manager whenever a policy issue has arisen. The extent of information that is included in the annotation/notification suggests or implies "a reason(s) for any validity check issues," since "corresponding result notification" would have suggested or implied to include information of any point of failures that have occurred during the execution of a policy, "so as to facilitate proper

follow up actions, such as rejection or acceptance of the e-mail message." (See, Final Office Action, pages 3-4; Emphasis in the original.)

The assignee respectfully disagrees with the office action's characterization of paragraphs 45-47 of Bandini. The "result notification" mentioned in Bandini is provided to ***the policy manager software module*** to facilitate follow-up actions. Even *assuming arguendo* that Bandini "suggests or implies" a reason for a validity check issue (which it does not), Bandini includes no teaching whatsoever of providing a reason for a validity check issue via ***a user interface on a mobile device***, as required by claim 26. Because in claim 26 the reason for the validity check issue is surfaced to the user, the user can take corrective action before the message is even sent.

The examiner further maintains that Bandini discloses "surfacing the validity check to the user so that the user can take corrective action before the message is even sent" based upon the following passage from paragraph 44: "[d]isposition action 620 determines whether the message should continue to the destination(s)." (See, Advisory Action dated June 16, 2008, page 2.) However contrary to this position, the "disposition action" at step 620 in the flowchart of figure 6(a) is being performed by the e-mail firewall and not by the user. This is made clear in multiple locations in Bandini: "FIG. 6(a) [which includes step 620] is a flowchart showing ***operation of the e-mail firewall*** 105 in response to a received message" (see, paragraph 43 of Bandini; emphasis added); and paragraph 15 of Bandini identifies figure 6(a) as "illustrating operation of the preferred embodiment of an e-mail firewall." Accordingly, any alleged corrective action in the cited passage of Bandini is being performed by the e-mail firewall and not by the user. Whether an electronic messaging reader is a type of user-interface (as maintained in the Advisory Action) is immaterial since, as shown above, Bandini discloses that it is the e-mail firewall performing the alleged corrective action and not the user. Since neither Bandini (nor

any of the other cited references) disclose the aforementioned limitation of claim 26, claim 26 is allowable and should proceed to issuance.

2. Neither Reference Teaches That The Processing Performed With Respect To A Secure Message Occurs Before A Message Is Even Sent.

Claim 26 of the instant application requires that processing of the secure message occurs before a message is even sent. This provides a user of the mobile device the benefit of taking steps to ameliorate the validity check issue before the secure message is ever sent.

Claim 26 makes clear that the processing of the secure message occurs before the message is sent, such as in the preamble (emphasis added): "*A wireless mobile communication device that handles a secure message to be sent from the wireless mobile communication device to a recipient*." Claim 26 further recites limitations about a secure message that is to be sent (i.e., the secure message has not been sent yet), such as the following limitation (emphasis added): "*means for using the stored certificate data to perform a validity check with respect to using the recipient's security key for sending the secure message to the recipient*."

The Final Office Action cites paragraph 44 of Bandini as disclosing this aspect of claim 26. However, paragraph 44 of Bandini is explicitly directed to the handling of e-mail messages that have already been sent by the user. Paragraph 44 discusses Figure 6(a) of Bandini. As Bandini states, "FIG. 6(a) is a flowchart showing operation of the e-mail firewall 105 in response to a ***received message***." (See, paragraph 43 of Bandini; emphasis added.) In Bandini, an e-mail firewall receives a message that has already been sent from a sender.

The Advisory Action further argues that processing is performed before a message is sent by maintaining that the processing of the message in Bandini is performed before it has been

delivered to the intended recipient. The assignee respectfully submits that this is an incorrect position. In general, a message is sent when a sender has activated the message send button and the message leaves the device. In Bandini, the e-mail message has already left the sender and is now being processed by the e-mail firewall as shown by the flowcharts of figures 6(a) and 6(b). Since neither Bandini (nor any of the other cited references) disclose the aforementioned feature of claim 26, claim 26 is allowable and should proceed to issuance.

F. Claim 27 Is Patentable Over Bandini and Baer

Claim 27 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Publication No. 2002/0169954, application of Bandini, et al. (Bandini) in view of U.S. Patent No. 6,782,266, issued to Baer, et al. (Baer). The rejection of claim 27 as being unpatentable over the cited references is improper because the cited references do not disclose the following limitations of claim 27:

- *using the received data to perform a validity check with respect to using the security key associated with the message recipient to send a secure message to the recipient;*
- *wherein the reason for the validity check issue is provided via a user interface on the mobile device.*

1. Neither Reference Teaches Claim 27's Limitation Of Providing A Reason For A Validity Check Issue Via A User Interface On A Mobile Device.

Claim 27 of the instant application is directed to handling on a wireless mobile communication device a secure message to be sent from the wireless mobile communication

device to a recipient. Claim 27 specifically recites that *the reason for the validity check issue is provided via a user interface on the mobile device*. In rejecting this subject matter of claim 27, the Final Office Action cites paragraph 44 of Bandini, which reads:

> Turning to FIG. 6(a), at 602, the e-mail firewall 105 determines if decryption of portions of the message 204 is required. If so, then at 604, decryption is performed in accordance with stored private keys 628. Storing private keys is well known in the art of public key cryptography. After decryption, or if no decryption is required, the e-mail firewall 105 applies policy managers 216, which can perform four types of actions (shown at 610, 612, 614, 616, and 620) on e-mail message 204 for each policy. Criteria actions 610 present filtering criteria selected by the administrator. Exception actions 612 determine which criteria 610 are excluded. Multiple criteria 610 can be selected which effectively results in a logical AND operation of the criteria. Multiple exceptions 612 can be selected which effectively results in a logical OR operation of the exceptions; that is, any one of the exception conditions being true will result in a policy not being triggered. In another embodiment, a generic Boolean expression is used in lieu of the criteria and exception combination. Annotation actions 614 cause generation of attachment to message 602 or insertion of text into the body 208 of the message. The manner by which annotations are made is based on a policy entered by the administrator. Notification actions 616 cause the sending of one or more e-mail notifications when a given policy is triggered. Notifications can be sent to sender, recipient, administrator, or any e-mail address that is defined by the administrator. In addition, notification actions 616 allow specification of whether the original message 204 should accompany the notification. Disposition action 620 determines whether the message should continue to the destination(s) (specified by field 620) or whether one of a plurality of alternative actions 622 such as deferral, quarantine, return to sender, or dropping of the message are required.

The cited passage, however, does not disclose the subject matter of claim 27, namely that a reason is determined for the issue resulting from the validity check and that reason is provided to the user of a mobile device. Bandini is only disclosing notification that an issue has arisen and does not provide any functionality for providing the underlying reason behind the issue. Because Bandini does not disclose a method of determining the reason for an issue that has arisen at the device and providing that reason to the user of a mobile device, the user has greater difficulty in

taking corrective action with respect to the issue. The simple notification in Bandini that an issue exists results in a significantly less efficient approach in allowing a mobile user to take ameliorative action, such as to take corrective action more quickly in order to allow the anticipated communication to take place once the issue is resolved.

The examiner "acknowledges" the assignee's concerns that Bandini does not disclose determining a reason for the issue resulting from the validity check. (See, Final Office Action, page 3.) However, the Final Office Action then cites paragraphs 45-47 of Bandini as teaching this limitation of claim 27, stating that the cited paragraphs provide "an example of a policy being triggered which provides further evidence of the extent of information that is included in the annotation and notification actions." (See, Final Office Action, page 3.) The office action's response to the assignee's argument further states:

> In the end of the execution of a policy being triggered, Bandini discloses that "the security manager provides a corresponding result notification to the policy manager so as to facilitate proper follow up actions, such as rejection or acceptance of the e-mail message (Par 0047)." This is evidence of the extent of information that is included in the Annotation, Notification actions of a Policy Manager whenever a policy issue has arisen. The extent of information that is included in the annotation/notification suggests or implies "a reason(s) for any validity check issues," since "corresponding result notification" would have suggested or implied to include information of any point of failures that have occurred during the execution of a policy, "so as to facilitate proper follow up actions, such as rejection or acceptance of the e-mail message." (See, Final Office Action, pages 3-4; Emphasis in the original.)

The assignee respectfully disagrees with the office action's characterization of paragraphs 45-47 of Bandini. The "result notification" mentioned in Bandini is provided to ***the policy manager software module*** to facilitate follow-up actions. Even *assuming arguendo* that Bandini "suggests or implies" a reason for a validity check issue (which it does not), Bandini includes no teaching whatsoever of providing a reason for a validity check issue via ***a user interface on a***

mobile device, as required by claim 27. Because in claim 27 the reason for the validity check issue is surfaced to the user, the user can take corrective action before the message is even sent.

The examiner further maintains that Bandini discloses "surfacing the validity check to the user so that the user can take corrective action before the message is even sent" based upon the following passage from paragraph 44: "[d]isposition action 620 determines whether the message should continue to the destination(s)." (See, Advisory Action dated June 16, 2008, page 2.) However contrary to this position, the "disposition action" at step 620 in the flowchart of figure 6(a) is being performed by the e-mail firewall and not by the user. This is made clear in multiple locations in Bandini: "FIG. 6(a) [which includes step 620] is a flowchart showing ***operation of the e-mail firewall*** 105 in response to a received message" (see, paragraph 43 of Bandini; emphasis added); and paragraph 15 of Bandini identifies figure 6(a) as "illustrating operation of the preferred embodiment of an e-mail firewall." Accordingly, any alleged corrective action in the cited passage of Bandini is being performed by the e-mail firewall and not by the user. Whether an electronic messaging reader is a type of user-interface (as maintained in the Advisory Action) is immaterial since, as shown above, Bandini discloses that it is the e-mail firewall performing the alleged corrective action and not the user. Since neither Bandini (nor any of the other cited references) disclose the aforementioned limitation of claim 27, claim 27 is allowable and should proceed to issuance.

2. Neither Reference Teaches That The Processing Performed With Respect To A Secure Message Occurs Before A Message Is Even Sent.

Claim 27 of the instant application requires that processing of the secure message occurs before a message is even sent. This provides a user of the mobile device the benefit of taking steps to ameliorate the validity check issue before the secure message is sent.

Claim 27 makes clear that the processing of the secure message occurs before the message is sent, such as in the preamble (emphasis added): "*... to perform a method for handling on a wireless mobile communication device a secure message that is to be sent from the wireless mobile communication device to a recipient.*" Claim 27 further recites operations about a secure message that is to be sent (i.e., the secure message has not been sent yet), such as the following (emphasis added): "*using the received data to perform a validity check with respect to using the security key associated with the message recipient to send a secure message to the recipient.*"

The Final Office Action cites paragraph 44 of Bandini as disclosing this aspect of claim 27. However, paragraph 44 of Bandini is explicitly directed to the handling of e-mail messages that have already been sent by the user. Paragraph 44 discusses Figure 6(a) of Bandini. As Bandini states, "FIG. 6(a) is a flowchart showing operation of the e-mail firewall 105 in response to a ***received message***." (See, paragraph 43 of Bandini; emphasis added.) In Bandini, an e-mail firewall receives a message that has already been sent from a sender.

The Advisory Action further argues that processing is performed before a message is sent by maintaining that the processing of the message in Bandini is performed before it has been delivered to the intended recipient. The assignee respectfully submits that this is an incorrect position. In general, a message is sent when a sender has activated the message send button and the message leaves the device. In Bandini, the e-mail message has already left the sender and is now being processed by the e-mail firewall as shown by the flowcharts of figures 6(a) and 6(b).

Since neither Bandini (nor any of the other cited references) disclose the aforementioned feature of claim 27, claim 27 is allowable and should proceed to issuance.

VIII. Claims Appendix

A claims appendix containing a copy of the claims subject to this appeal is attached.

IX. Evidence Appendix

No evidence is being submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132, nor is there any other evidence entered by the Examiner or relied upon by the Applicant. An evidence appendix indicating "None" is attached.

X. Related Proceedings Appendix

There are no related proceedings. A related proceedings appendix indicating "None" is attached.

Respectfully submitted,

Date: March 5, 2009

By: 

John V. Biernacki, Reg. No. 40,511
Jones Day
North Point
901 Lakeside Ave.
Cleveland, Ohio 44114
(216) 586-3939

CLAIMS APPENDIX

1. (Previously Presented) A method for handling on a wireless mobile communication device a secure message to be sent from the wireless mobile communication device to a recipient, comprising the steps of:

receiving data at the wireless mobile communication device about a security key associated with the recipient;

using the received data to perform a validity check with respect to using the security key associated with the recipient to send a secure message to the recipient;

wherein an issue exists due to the validity check;

determining a reason for the validity check issue;

wherein the reason for the validity check issue is provided via a user interface on the mobile device.

2. (Previously Presented) The method of claim 1, wherein a message is provided via the user interface indicating that a problem exists with respect to sending the secure message to the recipient in addition to indicating the reason related to the problem.

3. (Previously Presented) The method of claim 1, further comprising the step of resolving the validity check issue through use of the information provided in the validity check reason, wherein the secure message is sent after resolution of the validity check issue by the user.

4. (Previously Presented) The method of claim 1, wherein the security key is a public key, wherein a user composes the secure message, wherein the composed message is to be encrypted using the recipient's public key.

5. (Previously Presented) The method of claim 4, further comprising the steps of:

creating a list of all recipients for the composed message;

receiving data about the recipients' public keys that includes certificate information associated with the recipients; and

performing the validity check with respect to the certificate information associated with the recipients.

6. (Previously Presented) The method of claim 1, further comprising the steps of:

determining whether a certificate for an intended recipient can be located;

providing as a validity check reason that the intended recipient's certificate was not located.

7. (Previously Presented) The method of claim 6 further comprising the step of removing a recipient whose certificate was not located before sending a secure message to another recipient.

8. (Previously Presented) The method of claim 6 further comprising the step of canceling sending the message to a recipient whose certificate was not located.

9. (Previously Presented) The method of claim 6, further comprising the step of:

determining whether the certificate for the intended recipient is locally available on the mobile device.

10. (Previously Presented) The method of claim 6, further comprising the step of:

determining whether the certificate for the intended recipient is remotely available.

11. (Previously Presented) The method of claim 5, further comprising the step of collating certificates that correspond to the recipients before performing the validity check.

12. (Previously Presented) The method of claim 6, wherein the message is to be encrypted using a Secure Multipurpose Internet Mail Extensions (S/MIME) scheme or a Pretty Good Privacy (PGP) scheme.

13. (Previously Presented) The method of claim 1, wherein the received data about the security key associated with the recipient includes whether a recipient's certificate is permitted to be used;

wherein the validity check issue indicates that the recipient's certificate is not permitted to be used.

14. (Previously Presented) The method of claim 13, wherein the data about whether the recipient's certificate is permitted to be used is based on a usage field contained in the certificate.

15. (Previously Presented) The method of claim 13, wherein the data about whether the recipient's certificate is permitted to be used is based on a control file installed on the mobile device that specifies which certificates are allowed to be used.

16. (Previously Presented) The method of claim 1, wherein the issue involves a validity check failure, said method further comprising the step of providing the reason of the validity check failure to the user interface on the mobile device.

17. (Previously Presented) The method of claim 1, wherein the received data about the security key associated with the recipient includes strength of the recipient's certificate; and

wherein the validity check issue is directed to whether the recipient's certificate is permitted to be used based upon the strength of the recipient's certificate.

18. (Previously Presented) The method of claim 1, wherein the received data about the security key associated with the recipient includes whether the recipient's certificate is trusted, and wherein a decision to include a recipient for a secure message is based upon whether the recipient's certificate is trusted.

19. (Previously Presented) The method of claim 1, wherein the received data about the security key associated with the recipient includes validity and revocation status of a recipient's

certificate, and wherein a decision to include the recipient for the secure message is based upon the validity and revocation status of the recipient's certificate.

20. (Previously Presented) The method of claim 1, wherein the message is sent to the recipient despite notification of the validity check issue.

21. (Original) The method of claim 1, wherein means for providing a wireless network and means for providing a message server are used to transmit the secure message from the mobile device.

22. (Original) The method of claim 1, wherein the mobile device is a handheld wireless mobile communications device or a personal digital assistant (PDA).

23. (Canceled)

24. (Canceled)

25. (Previously Presented) An apparatus for handling on an electronic device a secure message to be sent from the electronic device to a recipient, comprising:

a secure message processing module for use with a messaging client that sends electronic messages to recipients;

wherein the secure message processing module receives data about a security key associated with the recipient;

wherein the secure message processing module uses the received data to perform a validity check with respect to using the security key associated with the recipient to send a secure message to the recipient;

wherein an issue exists based upon the validity check;

wherein the secure message processing module is configured to determine a reason for the validity check issue; and

wherein the secure message processing module provides the reason for the validity check issue via a user interface of the electronic device.

26. (Previously Presented) A wireless mobile communication device that handles a secure message to be sent from the wireless mobile communication device to a recipient, comprising:

a certificate store to store certificate data;

means for using the stored certificate data to perform a validity check with respect to using the recipient's security key for sending the secure message to the recipient;

wherein an issue exists due to the validity check;

means for determining a reason for the validity check issue; and

means for providing the reason for the validity check issue via a user interface of the mobile device.

27. (Previously Presented) A computer-readable storage medium encoded with instructions that cause a processor to perform a method for handling on a wireless mobile communication device a secure message that is to be sent from the wireless mobile communication device to a recipient, said method comprising:

receiving data at the wireless mobile communication device about a security key associated with the recipient;

using the received data to perform a validity check with respect to using the security key associated with the message recipient to send a secure message to the recipient;

wherein an issue exists due to the validity check;

determining a reason for the validity check issue;

wherein the reason for the validity check issue is provided via a user interface on the mobile device.

EVIDENCE APPENDIX

NONE

(No evidence is being submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132, nor is there any other evidence entered by the Examiner or relied upon by the Applicant)

RELATED PROCEEDINGS APPENDIX

NONE

(There are no related proceedings)